ΜΕΛΕΤΗ
ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ

[ΕΠΩΝΥΜΙΑ ΥΠΕΥΘΥΝΟΥ ΕΠΕΞΕΡΓΑΣΙΑΣ]

[ΤΙΤΛΟΣ ΕΞΕΤΑΖΟΜΕΝΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ]

Περιεχόμενα

Πρόλογος

Η παρούσα Μελέτη Εκτίμησης Αντικτύπου για την Προστασία των Δεδομένων Προσωπικού Χαρακτήρα (εφεξής εν συντομία αναφερόμενη ως «ΕΑΠΔ») διενεργείται στο πλαίσιο συμμόρφωσης με τις διατάξεις των άρθρων 35 και 36 του Γενικού Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (εφεξής εν συντομία αναφερόμενος ως «ΓΚΠΔ»).

Για την σύνταξη της παρούσας ΕΑΠΔ υιοθετήθηκε η πανευρωπαϊκά κοινώς αποδεκτή μεθοδολογία της Γαλλικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα «CNIL», η οποία περιλαμβάνει τρεις οδηγούς: (α) έναν που καθορίζει την προσέγγιση, (β) έναν δεύτερο που περιλαμβάνει γεγονότα που θα μπορούσαν να χρησιμοποιηθούν για να ενταχθεί σε κανόνες η ανάλυση και (γ) έναν τρίτο που παρέχει βάσεις γνώσεων και έναν κατάλογο μέτρων που στοχεύουν στη συμμόρφωση με τις νομικές υποχρεώσεις και την αντιμετώπιση των κινδύνων, καθώς και παραδείγματα.

Οι οδηγοί αυτοί μπορούν να ληφθούν από την ιστοσελίδα της CNIL :

https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual

1 Μελέτη του πλαισίου:

1.1 Επισκόπηση της επεξεργασίας

Περιγραφή της υπό εξέταση επεξεργασίας

Περιγραφή της επεξεργασίας[1]	
Σκοποί της επεξεργασίας	
Διακυβεύματα επεξεργασίας	
Υπεύθυνος επεξεργασίας	
Εκτελών-ούντες την επεξεργασία	

Ειδικά πρότυπα για κάθε τομέα τα οποία εφαρμόζονται στην επεξεργασία[2]

Πρότυπα που εφαρμόζονται στην επεξεργασία	Λήψη υπόψη

1.2 Προσωπικά δεδομένα, επεξεργασίες και υποστηρικτικά περιουσιακά στοιχεία

Περιγραφή των προσωπικών δεδομένων, αποδέκτες και διάρκειες αποθήκευσης

Κατηγορίες δεδομένων	Αποδέκτες	Διάρκεια αποθήκευσης

Περιγραφή των επεξεργασιών και των υποστηρικτικών στοιχείων

[εισάγετε ένα διάγραμμα ροών δεδομένων και μια λεπτομερή περιγραφή των επεξεργασιών που πραγματοποιούνται]

Επεξεργασίες	Λεπτομερής περιγραφή της επεξεργασίας	Υποστηρικτικά στοιχεία

[1] Η φύση της, το πεδίο εφαρμογής της, το πλαίσιό της, *κ.λπ.*
[2] Εγκεκριμένοι Κώδικες Δεοντολογίας κατά το άρθρο 40 - Βλέπε Άρθρο 35 παράγραφος 8 του [ΓΚΠΔ].

2 Μελέτη των θεμελιωδών αρχών:

2.1 Αξιολόγηση των μέτρων που εγγυώνται την αναλογικότητα και την αναγκαιότητα της επεξεργασίας

Εξήγηση και δικαιολόγηση των σκοπών

Σκοποί	Νομιμότητα

Εξήγηση και δικαιολόγηση της νόμιμης βάσης

Κριτήρια νομιμότητας	Εφαρμόσιμη	Δικαιολόγηση
Το υποκείμενο των δεδομένων έχει συναινέσει[3] στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς		
Η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης		
Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας		
Η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου		
Η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας		
Η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί[4]		

[3] Όσον αφορά στη λήψη της συγκατάθεσης του υποκειμένου των δεδομένων και την ενημέρωσή του, βλέπε Κεφάλαιο 2.2.
[4] Το σημείο αυτό δεν εφαρμόζεται στην επεξεργασία που πραγματοποιείται από δημόσιες αρχές κατά την εκτέλεση των καθηκόντων τους.

Εξήγηση και δικαιολόγηση της ελαχιστοποίησης των προσωπικών δεδομένων

Λεπτομέρειες για τα υπό επεξεργασία δεδομένα	Κατηγορίες δεδομένων	Δικαιολόγηση των αναγκών και της σχετικότητας των δεδομένων	Μέτρα ελαχιστοποίησης

Εξήγηση και δικαιολόγηση της ποιότητας των προσωπικών δεδομένων

Μέτρα για την ποιότητα των δεδομένων	Νομιμότητα

Εξήγηση και δικαιολόγηση της διάρκειας αποθήκευσης

Τύποι δεδομένων	Διάρκεια αποθήκευσης	Δικαιολόγηση της διάρκειας αποθήκευσης	Μηχανισμός διαγραφής στο τέλος της διάρκειας αποθήκευσης
Κοινά δεδομένα			
Αρχειοθετημένα δεδομένα			
Λειτουργικά ίχνη			
Τεχνικά αρχεία καταγραφής logs			

Αξιολόγηση των μέτρων

Μέτρα που εγγυώνται την αναλογικότητα και την αναγκαιότητα της επεξεργασίας	Αποδεκτό / μπορεί να βελτιωθεί;	Διορθωτικά μέτρα
Σκοποί: καθορισμένοι, ρητοί και νόμιμοι		
Βάση: νομιμότητα της επεξεργασίας, απαγόρευση της κατάχρησης		
Ελαχιστοποίηση δεδομένων: κατάλληλα, συναφή και περιορισμένα		
Ποιότητα δεδομένων: ακριβή και διατηρούμενα επικαιροποιημένα		
Διάρκεια αποθήκευσης: περιορισμένη		

2.2 Αξιολόγηση των μέτρων που προστατεύουν τα δικαιώματα των υποκειμένων των δεδομένων

Προσδιορισμός και περιγραφή των μέτρων για πληροφορίες για τα υποκείμενα των δεδομένων

Εάν η επεξεργασία επωφελείται από μια εξαίρεση από το δικαίωμα στην πληροφόρηση, όπως προβλέπεται στα Άρθρα 12, 13 και 14 του [ΓΚΠΔ]:

Εξαίρεση από την υποχρέωση ενημέρωσης των υποκειμένων των δεδομένων	Δικαιολόγηση

Διαφορετικά:

Μέτρα για το δικαίωμα στην πληροφόρηση	Υλοποίηση	Δικαιολόγηση της υλοποίησης ή της μη υλοποίησης
Παρουσίαση των όρων και συνθηκών χρήσης / εμπιστευτικότητας		
Δυνατότητα πρόσβασης στους όρους και συνθήκες χρήσης / εμπιστευτικότητας		
Ευανάγνωστοι και εύκολα κατανοητοί όροι		
Ύπαρξη ρητρών συγκεκριμένων για τη συσκευή		
Λεπτομερής παρουσίαση των σκοπών επεξεργασίας δεδομένων (CNIL) καθορισμένοι στόχοι, αντιστοίχιση δεδομένων κατά περίπτωση, *κ.λπ.*)		
Λεπτομερής παρουσίαση των συλλεγόμενων προσωπικών δεδομένων		
Παρουσίαση οποιασδήποτε πρόσβασης στα αναγνωριστικά της συσκευής, του smartphone / tablet ή του υπολογιστή, διευκρινίζοντας εάν αυτά τα αναγνωριστικά γνωστοποιούνται σε τρίτους		
Παρουσίαση των δικαιωμάτων του χρήστη ανάκληση συγκατάθεσης, διαγραφή δεδομένων, *κ.λπ.*		
Πληροφορίες σχετικά με τη μέθοδο ασφαλούς αποθήκευσης δεδομένων, ιδίως σε περίπτωση εξωτερικής ανάθεσης		
Ρυθμίσεις επικοινωνίας με την εταιρεία στοιχεία ταυτότητας και επικοινωνίας σχετικά με θέματα εμπιστευτικότητας		

Κατά περίπτωση, πληροφορίες για τον χρήστη σχετικά με οποιαδήποτε αλλαγή αφορά τα δεδομένα που συλλέγονται, τους σκοπούς και τις ρήτρες εμπιστευτικότητας		

Μέτρα για το δικαίωμα στην πληροφόρηση	Υλοποίηση	Δικαιολόγηση της υλοποίησης ή της μη υλοποίησης
Όσον αφορά στη διαβίβαση δεδομένων σε τρίτους:		
• λεπτομερής παρουσίαση των σκοπών της μετάδοσης σε τρίτους		
• λεπτομερής παρουσίαση των διαβιβαζόμενων προσωπικών δεδομένων		
• ένδειξη της ταυτότητας τρίτων φορέων		

Προσδιορισμός και περιγραφή των μέτρων για τη λήψη συγκατάθεσης[5]

Μέτρα για τη λήψη συγκατάθεσης	Υλοποίηση	Δικαιολόγηση της υλοποίησης ή της μη υλοποίησης
Ρητή συγκατάθεση κατά την εγγραφή		
Η συγκατάθεση κατανέμεται ανά κατηγορία δεδομένων ή τύπο επεξεργασίας		
Ρητή συγκατάθεση πριν από την ανταλλαγή δεδομένων με άλλους χρήστες		
Η συγκατάθεση παρουσιάζεται σε κατανοητή και εύκολα προσπελάσιμη μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα προσαρμοσμένη στον χρήστη – στόχο ιδιαίτερα για τα παιδιά		
Λήψη συγκατάθεσης των γονέων για ανηλίκους κάτω των 13 ετών		
Για έναν νέο χρήστη, πρέπει να ληφθεί εκ νέου η συγκατάθεση		
Μετά από μακρά περίοδο χωρίς χρήση, πρέπει να ζητηθεί από το χρήστη να επιβεβαιώσει τη συγκατάθεσή του		
Εάν ο χρήστης έχει συναινέσει στην επεξεργασία ειδικών δεδομένων π.χ. τη θέση του), η διεπαφή δηλώνει σαφώς ότι λαμβάνει χώρα η εν λόγω επεξεργασία εικονίδιο, ενδεικτική λυχνία		
Εάν ο χρήστης αλλάξει συσκευή, smartphone ή υπολογιστή, επανεγκαταστήσει την εφαρμογή για κινητά, ή διαγράψει τα cookies του, διατηρούνται οι ρυθμίσεις που σχετίζονται με τη συγκατάθεσή του		

[5] Όταν νόμιμη βάση της επεξεργασίας είναι η συγκατάθεση.

Προσδιορισμός και περιγραφή των μέτρων για τα δικαιώματα πρόσβασης και φορητότητας δεδομένων

Όταν η επεξεργασία επωφελείται από εξαίρεση από το δικαίωμα πρόσβασης, όπως προβλέπεται στο άρθρο 15 του [ΓΚΠΔ]:

Εξαίρεση από το δικαίωμα στην πρόσβαση	Δικαιολόγηση	Μέθοδοι ανταπόκρισης στα υποκείμενα των δεδομένων

Διαφορετικά:

Μέτρα για το δικαίωμα πρόσβασης	Εσωτερικά δεδομένα	Εξωτερικά δεδομένα	Δικαιολόγηση
Δυνατότητα πρόσβασης σε όλα τα προσωπικά δεδομένα του χρήστη, μέσω των κοινών διεπαφών			
Δυνατότητα ασφαλούς εξέτασης των ιχνών χρήσης που σχετίζονται με τον χρήστη			
Δυνατότητα λήψης ενός αρχείου όλων των προσωπικών δεδομένων που σχετίζονται με τον χρήστη			

Τέλος, όταν το δικαίωμα στη φορητότητα δεδομένων ισχύει για την επεξεργασία σύμφωνα με το άρθρο 20 του [ΓΚΠΔ]:

Μέτρα για το δικαίωμα φορητότητας	Εσωτερικά δεδομένα	Εξωτερικά δεδομένα	Δικαιολόγηση
Δυνατότητα ανάκτησης, σε μορφή εύκολα επαναχρησιμοποιήσιμη, προσωπικών δεδομένων που παρασχέθηκαν από τον χρήστη, έτσι ώστε να μεταφερθούν σε άλλη υπηρεσία			

Προσδιορισμός και περιγραφή των μέτρων για τα δικαιώματα διόρθωσης και διαγραφής

Όταν η επεξεργασία επωφελείται από απαλλαγή από το δικαίωμα διόρθωσης και διαγραφής, όπως προβλέπεται στο Άρθρο 17 του [ΓΚΠΔ]:

Εξαίρεση από τα δικαιώματα στη διόρθωση και διαγραφή	Δικαιολόγηση	Μέθοδοι ανταπόκρισης στα υποκείμενα των δεδομένων

Διαφορετικά:

Μέτρα για τα δικαιώματα διόρθωσης και διαγραφής	Εσωτερικά δεδομένα	Εξωτερικά δεδομένα	Δικαιολόγηση
Δυνατότητα διόρθωσης προσωπικών δεδομένων			
Δυνατότητα διαγραφής προσωπικών δεδομένων			
Υποδήλωση των προσωπικών δεδομένων που σε κάθε περίπτωση θα αποθηκευτούν τεχνικές απαιτήσεις, νομικές υποχρεώσεις *κ.λπ.*)			
Εφαρμογή του δικαιώματος στη λήθη για ανηλίκους			
Ξεκάθαρες ενδείξεις και απλά βήματα για τη διαγραφή δεδομένων πριν από την απόσυρση της συσκευής			
Συμβουλές που δίνονται σχετικά με την επαναφορά ρυθμίσεων της συσκευής πριν την πώλησή της			
Δυνατότητα διαγραφής δεδομένων σε περίπτωση κλοπής της συσκευής			

Προσδιορισμός και περιγραφή των μέτρων για τα δικαιώματα στον περιορισμό της επεξεργασίας και στην εναντίωση

Εάν η επεξεργασία επωφελείται από μια εξαίρεση από το δικαίωμα στον περιορισμό της επεξεργασίας και στην εναντίωση, όπως προβλέπεται στο Άρθρο 38 του [DP-Act] ή στο Άρθρο 21 του [ΓΚΠΔ]:

Εξαίρεση από το δικαίωμα στον περιορισμό της επεξεργασίας και στην εναντίωση	Δικαιολόγηση	Μέθοδοι για την ανταπόκριση στα υποκείμενα των δεδομένων

Διαφορετικά:

Μέτρα για τα δικαιώματα στον περιορισμό της επεξεργασίας και στην εναντίωση	Εσωτερικά δεδομένα	Εξωτερικά δεδομένα	Δικαιολόγηση
Ύπαρξη ρυθμίσεων «Απορρήτου»			
Πρόσκληση για αλλαγή των προεπιλεγμένων ρυθμίσεων			
Οι ρυθμίσεις «Απορρήτου» είναι προσβάσιμες κατά την εγγραφή			
Οι ρυθμίσεις «Απορρήτου» είναι προσβάσιμες μετά την εγγραφή			
Ύπαρξη συστήματος γονικού ελέγχου για παιδιά κάτω των 13 ετών			
Συμμόρφωση όσον αφορά στην παρακολούθηση cookies, διαφήμιση, *κ.λπ.*)			
Αποκλεισμός παιδιών ηλικίας κάτω των 13 ετών από αυτοματοποιημένο προφίλ			
Αποτελεσματικός αποκλεισμός της επεξεργασίας των δεδομένων του χρήστη στην περίπτωση που η συγκατάθεσή του ανακληθεί			

Προσδιορισμός και περιγραφή των μέτρων που αφορούν στους εκτελούντες την επεξεργασία

Όνομα εκτελούντος την επεξεργασία	Σκοπός	Πεδίο εφαρμογής	Αναγνωριστικό σύμβασης	Συμμόρφωση με το Άρθρο 28[6]

[6] Πρέπει να υπογραφεί μια σύμβαση επεξεργασίας με κάθε εκτελούντα την επεξεργασία, η οποία θα περιλαμβάνει όλες τις πτυχές που προβλέπονται στο Άρθρο 28 του [ΓΚΠΔ]: διάρκεια, πεδίο εφαρμογής, σκοπός, καταγεγραμμένες οδηγίες επεξεργασίας, προηγούμενη άδεια αν προσληφθεί άλλος εκτελών την επεξεργασία, παροχή οποιασδήποτε τεκμηρίωσης που αποδεικνύει τη συμμόρφωση με τον [ΓΚΠΔ], άμεση κοινοποίηση οποιασδήποτε παραβίασης των δεδομένων, *κ.λπ.*

Προσδιορισμός και περιγραφή των μέτρων για τη διαβίβαση δεδομένων εκτός της Ευρωπαϊκής Ένωσης

Σύνολα δεδομένων και θέση αποθήκευσης	Ελλάδα	ΕΕ	Χώρα που αναγνωρίζεται ότι προσφέρει επαρκή προστασία από την ΕΕ	Άλλη χώρα	Δικαιολόγηση και εποπτεία (CNIL) τυποποιημένες συμβατικές ρήτρες, εσωτερικοί εταιρικοί κανονισμοί)

Αξιολόγηση των μέτρων

Μέτρα για την προστασία δικαιωμάτων των υποκειμένων των δεδομένων	Αποδεκτό / μπορεί να βελτιωθεί;	Διορθωτικά μέτρα
Πληροφορίες για τα υποκείμενα των δεδομένων δίκαιη και διαφανής επεξεργασία)		
Λήψη συγκατάθεσης		
Εφαρμογή των δικαιωμάτων πρόσβασης και φορητότητας		
Εφαρμογή των δικαιωμάτων διόρθωσης και διαγραφής		
Εφαρμογή του δικαιώματος περιορισμού της επεξεργασίας και του δικαιώματος αντίρρησης		
Εκτελούντες την επεξεργασία: προσδιορισμένοι και διεπόμενοι από σύμβαση		
Διαβιβάσεις: συμμόρφωση με τις υποχρεώσεις που αφορούν στη διαβίβαση δεδομένων εκτός της Ευρωπαϊκής Ένωσης		

3 Μελέτη των κινδύνων που σχετίζονται με την ασφάλεια των δεδομένων:

3.1 Αξιολόγηση των μέτρων ασφάλειας

Περιγραφή και αξιολόγηση των μέτρων που εφαρμόζονται για την αντιμετώπιση των κινδύνων που είναι σχετικοί με την ασφάλεια προσωπικών δεδομένων

Μέτρα που αφορούν ειδικά στα υπό επεξεργασία δεδομένα	Υλοποίηση ή δικαιολόγηση της έλλειψής της	Αποδεκτό / μπορεί να βελτιωθεί;	Διορθωτικά μέτρα
Κρυπτογράφηση	*[Περιγράψτε εδώ τα μέσα που εφαρμόζονται για τη διασφάλιση της εμπιστευτικότητας των αποθηκευμένων δεδομένων (στη βάση δεδομένων, στα επίπεδα αρχεία, στα αντίγραφα ασφαλείας, κ.λπ.), καθώς και για τη διαδικασία διαχείρισης κλειδιών κρυπτογράφησης (δημιουργία, αποθήκευση, αλλαγή σε περίπτωση υποψίας περιστατικού παραβίασης δεδομένων κ.λπ.). Περιγράψτε τα μέσα κρυπτογράφησης που χρησιμοποιούνται για τις ροές δεδομένων (VPN, TLS, κ.λπ.) τα οποία εφαρμόζονται στην επεξεργασία.]*		
Ανωνυμοποίηση	*[Αναφέρετε εδώ εάν εφαρμόζονται μηχανισμοί ανωνυμοποίησης, ποιοι και για ποιο σκοπό.]*		
Κατάτμηση δεδομένων (σχετικά με το υπόλοιπο του πληροφοριακού συστήματος)	*[Αναφέρετε εδώ εάν η κατάτμηση της επεξεργασίας είναι προγραμματισμένη και πώς γίνεται αυτή.]*		
Έλεγχος λογικής πρόσβασης	*[Περιγράψτε εδώ αν τα προφίλ των χρηστών ορίζονται και αποδίδονται. Διευκρινίστε τα μέσα ελέγχου ταυτότητας που εφαρμόζονται. Κατά περίπτωση, διευκρινίστε τους κανόνες που ισχύουν για τους κωδικούς πρόσβασης (ελάχιστο μήκος, απαιτούμενοι χαρακτήρες, διάρκεια ισχύος, αριθμός αποτυχημένων προσπαθειών πριν κλειδωθεί η πρόσβαση στον λογαριασμό, κ.λπ.).]*		

Μέτρα που αφορούν ειδικά στα υπό επεξεργασία δεδομένα	Υλοποίηση ή δικαιολόγηση της έλλειψής της	Αποδεκτό / μπορεί να βελτιωθεί;	Διορθωτικά μέτρα
Ιχνηλασιμότητα (καταγραφή συμβάντων)	*[Υποδείξτε εδώ αν τα συμβάντα καταγράφονται και για πόσο χρόνο αποθηκεύονται αυτά τα ίχνη.]*		
Παρακολούθηση ακεραιότητας	*[Υποδείξτε εδώ αν εφαρμόζονται μηχανισμοί για την παρακολούθηση της ακεραιότητας των αποθηκευμένων δεδομένων, ποιοι και για ποιο σκοπό.* *Καθορίστε ποιοι μηχανισμοί ελέγχου της ακεραιότητας εφαρμόζονται στις ροές δεδομένων.]*		
Αρχειοθέτηση	*[Περιγράψτε εδώ τις διαδικασίες διαχείρισης αρχείων (παράδοση, αποθήκευση, πρόσβαση, κ.λπ.) υπό την ευθύνη σας. Καθορίστε τους ρόλους αρχειοθέτησης (γραφεία προέλευσης, υπηρεσίες που διαβιβάζουν, κ.λπ.) και την πολιτική αρχειοθέτησης.* *Αναφέρετε εάν τα δεδομένα ενδέχεται να εμπίπτουν στα δημόσια αρχεία.]*		
Ασφάλεια έγχαρτων εγγράφων	*[Εάν κατά τη διάρκεια της επεξεργασίας χρησιμοποιούνται έγχαρτα έγγραφα που περιέχουν δεδομένα, υποδείξτε εδώ τον τρόπο εκτύπωσης, αποθήκευσης, καταστροφής και ανταλλαγής τους.]*		

Περιγραφή και αξιολόγηση των μέτρων για τη γενική ασφάλεια

Μέτρα για την γενική ασφάλεια σχετικά με το σύστημα στο οποίο γίνεται η επεξεργασία	Υλοποίηση ή δικαιολόγηση της έλλειψής της	Αποδεκτό / μπορεί να βελτιωθεί;	Διορθωτικά μέτρα
Λειτουργική ασφάλεια	*[Περιγράψτε εδώ πώς πραγματοποιούνται οι ενημερώσεις λογισμικού (λειτουργικά συστήματα, εφαρμογές, κ.λπ.) και η εφαρμογή διορθωτικών μέτρων ασφάλειας.]*		
Καταπολέμηση κακόβουλου λογισμικού	*[Δηλώστε εδώ εάν λογισμικό προστασίας από ιούς είναι εγκατεστημένο και ενημερώνεται σε τακτά χρονικά διαστήματα στους σταθμούς εργασίας.]*		
Διαχείριση σταθμών εργασίας	*[Περιγράψτε εδώ τα μέτρα που εφαρμόζονται σε σταθμούς εργασίας (αυτόματο κλείδωμα, τείχος προστασίας, κ.λπ.).]*		
Ασφάλεια ιστότοπου	*[Αναφέρετε εδώ εάν έχουν εφαρμοστεί οι συστάσεις για την ασφάλεια ιστοσελίδων» της ANSSI.]*		
Αντίγραφα ασφαλείας	*[Υποδείξτε εδώ τον τρόπο διαχείρισης των αντιγράφων ασφαλείας. Διευκρινίστε εάν αποθηκεύονται σε ασφαλές μέρος.]*		
Συντήρηση	*[Περιγράψτε εδώ πώς γίνεται η διαχείριση της φυσικής συντήρησης του υλισμικού και αν αυτή έχει ανατεθεί με σύμβαση.* *Υποδείξτε εάν επιτρέπεται η απομακρυσμένη συντήρηση εφαρμογών και σύμφωνα με ποιες ρυθμίσεις.* *Καθορίστε εάν γίνεται διαχείριση του ελαττωματικού εξοπλισμού με έναν συγκεκριμένο τρόπο.]*		
Ασφάλεια διαύλων πληροφορίας (δίκτυα)	*[Υποδείξτε εδώ τον τύπο του δικτύου στο οποίο πραγματοποιείται η επεξεργασία (απομονωμένο, ιδιωτικό ή Διαδίκτυο).*		

Μέτρα για την γενική ασφάλεια σχετικά με το σύστημα στο οποίο γίνεται η επεξεργασία	Υλοποίηση ή δικαιολόγηση της έλλειψής της	Αποδεκτό / μπορεί να βελτιωθεί;	Διορθωτικά μέτρα
Ασφάλεια διαύλων πληροφορίας δίκτυα	*Καθορίστε ποιο σύστημα τείχους προστασίας, συστήματα ανίχνευσης εισβολών ή άλλοι ενεργοί ή παθητικοί μηχανισμοί είναι υπεύθυνοι για τη διασφάλιση του δικτύου.]*		
Παρακολούθηση	*[Αναφέρετε εδώ αν υλοποιείται παρακολούθηση τοπικών δικτύων σε πραγματικό χρόνο και με ποια μέσα.* *Αναφέρετε εάν πραγματοποιείται παρακολούθηση των διαμορφώσεων υλισμικού και λογισμικού και με ποια μέσα.]*		
Έλεγχος φυσικής πρόσβασης	*[Αναφέρετε εδώ πώς διεξάγεται ο φυσικός έλεγχος πρόσβασης όσον αφορά στους χώρους που εξυπηρετούν την επεξεργασία (χωρισμός σε ζώνες, συνοδεία επισκεπτών, ένδυση με πάσο, κλειδωμένες πόρτες, κ.ο.κ.).* *Αναφέρετε εάν υπάρχουν διαδικασίες προειδοποίησης σε περίπτωση διάρρηξης.]*		
Ασφάλεια υλισμικού	*[Αναφέρετε εδώ τα μέτρα που αφορούν στη φυσική ασφάλεια των διακομιστών και των σταθμών εργασίας που ανήκουν σε πελάτες (ασφαλής αποθήκευση, καλώδια ασφαλείας, φίλτρα εμπιστευτικότητας, ασφαλής διαγραφή πριν από την απόσυρση, κ.λπ.).]*		
Αποφυγή πηγών κινδύνου	*[Αναφέρετε εδώ εάν η περιοχή εγκατάστασης υπόκειται σε περιβαλλοντικές καταστροφές (ζώνη πλημμυρών, γειτνίαση με χημικές βιομηχανίες, σεισμική ή ηφαιστειακή ζώνη, κλπ.).* *Καθορίστε εάν επικίνδυνα προϊόντα αποθηκεύονται στην ίδια περιοχή.]*		

Μέτρα για την γενική ασφάλεια σχετικά με το σύστημα στο οποίο γίνεται η επεξεργασία	Υλοποίηση ή δικαιολόγηση της έλλειψής της	Αποδεκτό / μπορεί να βελτιωθεί;	Διορθωτικά μέτρα
Προστασία έναντι πηγών κινδύνου που δεν προέρχονται από ανθρώπους	*[Περιγράψτε εδώ τους τρόπους πρόληψης, ανίχνευσης και καταπολέμησης της φωτιάς.* *Κατά περίπτωση, αναφέρετε τα μέσα πρόληψης της ζημιάς από νερό.* *Προσδιορίστε επίσης τα μέσα παρακολούθησης της τροφοδοσίας και εξασφάλισης τροφοδοσίας ηλεκτρικού ρεύματος.]*		

Περιγραφή και αξιολόγηση των οργανωτικών μέτρων (διακυβέρνηση)

Οργανωτικά μέτρα (διακυβέρνηση)	Υλοποίηση ή δικαιολόγηση της έλλειψής της	Αποδεκτό / μπορεί να βελτιωθεί;	Διορθωτικά μέτρα
Οργάνωση	*[Αναφέρατε αν είναι καθορισμένοι οι ρόλοι και οι ευθύνες για την προστασία προσωπικών δεδομένων.* *Καθορίστε εάν ένα πρόσωπο είναι υπεύθυνο για την εφαρμογή των νόμων και των κανονισμών περί ιδιωτικότητας.* *Καθορίστε εάν υπάρχει επιτροπή παρακολούθησης (ή ισοδύναμη) υπεύθυνη για την καθοδήγηση και την παρακολούθηση των δράσεων που αφορούν στην προστασία της ιδιωτικότητας.]*		
Πολιτική (διαχείριση των κανόνων)	*[Υποδείξτε εάν υπάρχει χάρτης ΤΠΕ (ή ισοδύναμος) σχετικά με την προστασία δεδομένων και τη σωστή χρήση των πόρων ΤΠΕ.]*		
Διαχείριση κινδύνων	*[Αναφέρετε εδώ εάν αξιολογούνται οι κίνδυνοι για την ιδιωτικότητα των υποκειμένων των δεδομένων που προκύπτουν από νέες επεξεργασίες, αν είναι συστηματικές ή όχι και, κατά περίπτωση, σύμφωνα με ποια μέθοδο.* *Προσδιορίστε εάν έχει καθιερωθεί η χαρτογράφηση των κινδύνων προστασίας της ιδιωτικότητας σε επίπεδο οργανισμού.]*		
Διαχείριση έργων	*[Υποδείξτε εδώ αν οι δοκιμές συσκευών εκτελούνται με πλασματικά / ανώνυμα δεδομένα.]*		
Διαχείριση περιστατικών και παραβιάσεων προσωπικών δεδομένων	*[Υποδείξτε εδώ αν περιστατικά ΤΠΕ υπόκεινται σε τεκμηριωμένη και δοκιμασμένη διαδικασία διαχείρισης.]*		
Διαχείριση προσωπικού	*[Υποδείξτε εδώ ποια μέτρα λαμβάνονται για την ευαισθητοποίηση των*		

Περιγραφή και αξιολόγηση των οργανωτικών μέτρων (διακυβέρνηση)

Μέτρα για τη γενική ασφάλεια σχετικά με το σύστημα στο οποίο γίνεται η επεξεργασία	Υλοποίηση ή δικαιολόγηση της έλλειψής της	Αποδεκτό / μπορεί να βελτιωθεί;	Διορθωτικά μέτρα
Διαχείριση προσωπικού	*προσφάτως προσληφθέντων.* *Υποδείξτε ποια μέτρα λαμβάνονται όταν άτομα που έχουν πρόσβαση σε δεδομένα αποχωρούν από τη θέση εργασίας τους.]*		
Σχέσεις με τρίτους	*[Υποδείξτε εδώ, για τους εκτελούντες την επεξεργασία που χρειάζονται πρόσβαση στα δεδομένα, τα μέτρα ασφαλείας και τις ρυθμίσεις που έχουν εφαρμοστεί όσον αφορά στην πρόσβαση αυτή.]*		
Επίβλεψη	*[Αναφέρατε εδώ εάν παρακολουθείται η αποτελεσματικότητα και η επάρκεια των μέτρων ιδιωτικότητας.]*		

3.2 Αξιολόγηση κινδύνων: πιθανές παραβιάσεις ιδιωτικότητας

Ανάλυση και αξιολόγηση των κινδύνων

Κίνδυνος	Κύριες πηγές κινδύνου	Κύριες απειλές	Κύριες πιθανές επιπτώσεις	Κύρια μέτρα που μειώνουν τη σοβαρότητα και την πιθανότητα	Σοβαρότητα	Πιθανότητα
Αθέμιτη πρόσβαση σε δεδομένα						
Ανεπιθύμητη τροποποίηση δεδομένων						
Εξαφάνιση δεδομένων						

Αξιολόγηση των κινδύνων

Κίνδυνοι	Αποδεκτό/ μπορεί να βελτιωθεί;	Διορθωτικά μέτρα	Υπολειπόμενη σοβαρότητα	Υπολειπόμενη πιθανότητα
Αθέμιτη πρόσβαση σε δεδομένα	*[Ο αξιολογητής πρέπει να καθορίσει εάν τα υπάρχοντα ή προγραμματισμένα μέτρα (που έχουν ήδη αναληφθεί) περιορίζουν επαρκώς αυτόν τον κίνδυνο ώστε να θεωρηθεί αποδεκτός.]*	*[Εφόσον συντρέχει περίπτωση, πρέπει να αναφέρει εδώ τυχόν πρόσθετα μέτρα που θα αποδειχθούν αναγκαία.]*		
Ανεπιθύμητη τροποποίηση δεδομένων	*[Ο αξιολογητής πρέπει να καθορίσει εάν τα υπάρχοντα ή προγραμματισμένα μέτρα (που έχουν ήδη αναληφθεί) περιορίζουν επαρκώς αυτόν τον κίνδυνο ώστε να θεωρηθεί αποδεκτός.]*	*[Εφόσον συντρέχει περίπτωση, πρέπει να αναφέρει εδώ τυχόν πρόσθετα μέτρα που θα αποδειχθούν αναγκαία.]*		
Εξαφάνιση δεδομένων	*[Ο αξιολογητής πρέπει να καθορίσει εάν τα υπάρχοντα ή προγραμματισμένα μέτρα (που έχουν ήδη αναληφθεί) περιορίζουν επαρκώς αυτόν τον κίνδυνο ώστε να θεωρηθεί αποδεκτός.]*	*[Εφόσον συντρέχει περίπτωση, πρέπει να αναφέρει εδώ τυχόν πρόσθετα μέτρα που θα αποδειχθούν αναγκαία.]*		

4 Επικύρωση της ΕΑΠΔ:

4.1 Προετοιμασία του υλικού που απαιτείται για την επικύρωση

Ανάπτυξη της σύνοψης σχετικά με τη συμμόρφωση με τον [ΓΚΠΔ] των μέτρων που επιλέχθηκαν για την τήρηση των θεμελιωδών αρχών

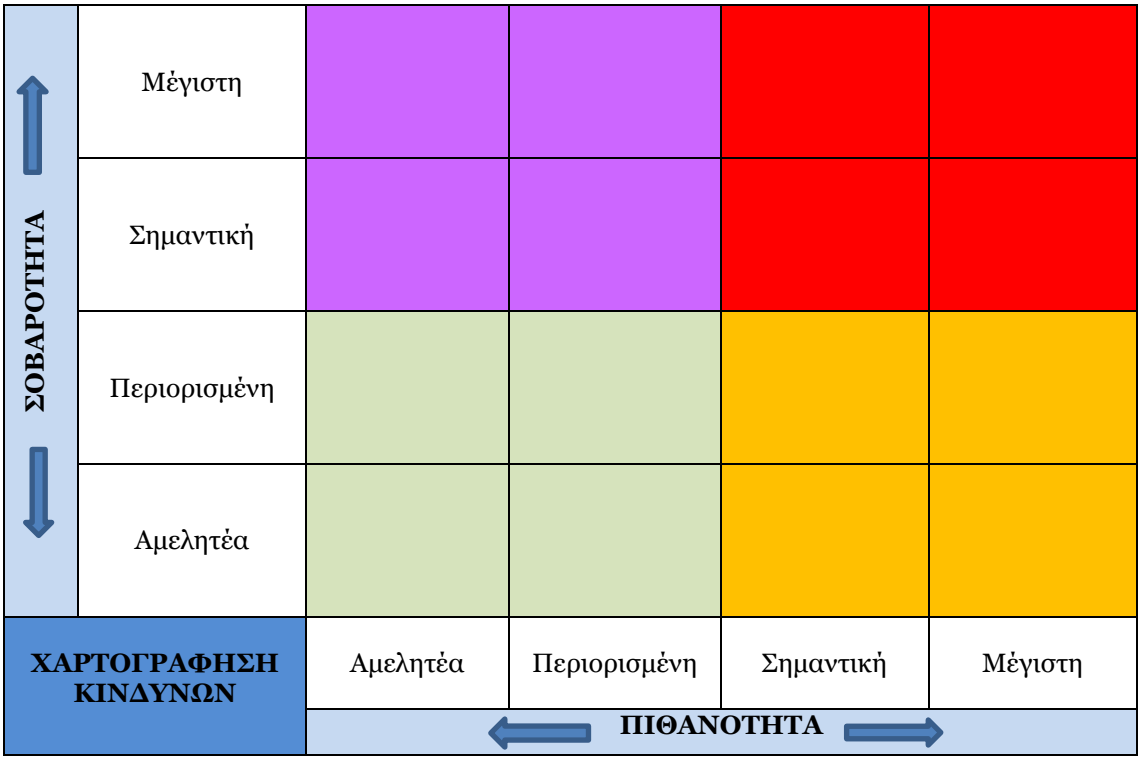
Ένδειξη				
Σύμβολο :	●●●	●○○	○●○	○○●
Νόημα :	Μη εφαρμοστέο	Μη ικανοποιητικό	Προγραμματισμένη βελτίωση	Αποδεκτό

Μέτρα επιλεγμένα για τη διασφάλιση της συμμόρφωσης με τις θεμελιώδεις αρχές	Αξιολόγηση
Μέτρα που εγγυώνται την αναλογικότητα και την αναγκαιότητα της επεξεργασίας	
Σκοπός-οι: καθορισμένος, ρητός και νόμιμος	○○○
Βάση: νομιμότητα της επεξεργασίας, απαγόρευση της κατάχρησης	○○○
Ελαχιστοποίηση δεδομένων: κατάλληλα, συναφή και περιορισμένα	○○○
Ποιότητα δεδομένων: ακριβή και επικαιροποιημένα	○○○
Διάρκεια αποθήκευσης: περιορισμένη	○○○
Μέτρα για την προστασία των προσωπικών δικαιωμάτων των υποκειμένων των δεδομένων	
Πληροφορίες για τα υποκείμενα των δεδομένων δίκαιη και διαφανής επεξεργασία	○○○
Λήψη συγκατάθεσης	○○○
Άσκηση του δικαιώματος πρόσβασης και του δικαιώματος μεταφοράς δεδομένων	○○○
Άσκηση των δικαιωμάτων διόρθωσης και διαγραφής	○○○
Άσκηση δικαιώματος περιορισμού της επεξεργασίας και δικαιώματος αντίρρησης	○○○
Εκτελούντες την επεξεργασία: προσδιορισμένοι και διεπόμενοι από σύμβαση	○○○
Διαβιβάσεις: συμμόρφωση με τις υποχρεώσεις που αφορούν στη διαβίβαση δεδομένων εκτός της Ευρωπαϊκής Ένωσης	○○○

Ανάπτυξη της σύνοψης σχετικά με τη συμμόρφωση με τις καλές πρακτικές των μέτρων που συμβάλλουν στην αντιμετώπιση των κινδύνων για την ασφάλεια των δεδομένων

Μέτρα εφαρμοσμένα για αντιμετώπιση των κινδύνων για την ασφάλεια δεδομένων	Αξιολόγηση
Μέτρα που αφορούν ειδικά στα δεδομένα που υφίστανται επεξεργασία	
Κρυπτογράφηση	ΟΟΟ
Ανωνυμοποίηση	ΟΟΟ
Κατάτμηση δεδομένων σχετικά με το υπόλοιπο του πληροφοριακού συστήματος	ΟΟΟ
Έλεγχος λογικής πρόσβασης	ΟΟΟ
Ιχνηλασιμότητα καταγραφή συμβάντων	ΟΟΟ
Παρακολούθηση ακεραιότητας	ΟΟΟ
Αρχειοθέτηση	ΟΟΟ
Ασφάλεια έγχαρτων εγγράφων	ΟΟΟ
Μέτρα για την γενική ασφάλεια του συστήματος στο οποίο πραγματοποιείται η επεξεργασία	
Λειτουργική ασφάλεια	ΟΟΟ
Καταπολέμηση κακόβουλου λογισμικού	ΟΟΟ
Διαχείριση σταθμών εργασίας	ΟΟΟ
Ασφάλεια ιστότοπου	ΟΟΟ
Αντίγραφα ασφαλείας	ΟΟΟ
Συντήρηση	ΟΟΟ
Ασφάλεια διαύλων πληροφορίας δίκτυα	ΟΟΟ
Παρακολούθηση	ΟΟΟ
Έλεγχος φυσικής πρόσβασης	ΟΟΟ
Ασφάλεια υλισμικού	ΟΟΟ
Αποφυγή πηγών κινδύνου	ΟΟΟ
Προστασία έναντι πηγών κινδύνου που δεν προέρχονται από ανθρώπους	ΟΟΟ
Οργανωτικά μέτρα διακυβέρνηση	
Οργάνωση	ΟΟΟ
Πολιτική διαχείριση των κανόνων	ΟΟΟ
Διαχείριση κινδύνων	ΟΟΟ
Διαχείριση έργων	ΟΟΟ
Διαχείριση περιστατικών και παραβιάσεων προσωπικών δεδομένων	ΟΟΟ
Διαχείριση προσωπικού	ΟΟΟ
Σχέσεις με τρίτους	ΟΟΟ
Επίβλεψη	ΟΟΟ

Χαρτογράφηση των κινδύνων που αφορούν στην ασφάλεια προσωπικών δεδομένων



Ανάπτυξη σχεδίου δράσης

Πρόσθετα μέτρα που ζητήθηκαν	Διευθυντής	Συχνότητα	Δυσκολία	Κόστος	Πρόοδος

Τεκμηρίωση των συμβουλών του επικεφαλής για θέματα «Προστασίας Δεδομένων»[7]

Την ημέρα / μήνα / έτος, ο Υπεύθυνος Προστασίας Δεδομένων της [επωνυμία εταιρείας] εξέδωσε την ακόλουθη γνώμη σχετικά με τη συμμόρφωση της επεξεργασίας και τη μελέτη Εκτίμησης Αντικτύπου που διενεργήθηκε:

[Υπογραφή]

Τεκμηρίωση της άποψης των υποκειμένων των δεδομένων ή των εκπροσώπων τους[8]

Τα υποκείμενα των δεδομένων [συμμετείχαν/ δεν συμμετείχαν] σε διαβούλευση [και εξέφρασαν την ακόλουθη άποψη σχετικά με τη συμμόρφωση της επεξεργασίας ενόψει της διεξαχθείσας μελέτης]:

Δικαιολόγηση της απόφασης του υπεύθυνου επεξεργασίας:

[7] Βλέπε Άρθρο 35 παράγραφος 2 του [ΓΚΠΔ].
[8] Βλέπε Άρθρο 35 παράγραφος 9 του [ΓΚΠΔ].

4.2 Επίσημη επικύρωση της ΕΑΠΔ

Τεκμηρίωση της επικύρωσης

Την ημέρα / μήνα / έτος, ο [τίτλος εκπροσώπου Υπεύθυνου Επεξεργασίας] της εταιρείας με την επωνυμία [XXXXXXX] επικυρώνει την παρούσα Μελέτη Εκτίμησης Αντικτύπου για την επεξεργασία του/της [τίτλος επεξεργασίας], υπό το πρίσμα της μελέτης που διεξήχθη, υπό την ιδιότητά του ως [υπεύθυνος επεξεργασίας].

Οι σκοποί της επεξεργασίας είναι να επιτραπεί στο υποκείμενο των δεδομένων να .....[υπενθύμιση του σκοπού επεξεργασίας].....

Αυτό οφείλεται στο γεγονός ότι τα μέτρα που σχεδιάζονται για τη συμμόρφωση με τις θεμελιώδεις αρχές που διέπουν την προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικότητας και για την αντιμετώπιση των κινδύνων που ελλοχεύουν για τα υποκείμενα των δεδομένων κρίθηκαν αποδεκτά σε σχέση με αυτά τα διακυβεύματα. Ωστόσο, θα πρέπει να αποδειχθεί η εφαρμογή πρόσθετων μέτρων, καθώς και η συνεχής βελτίωση της Μελέτης Εκτίμησης Αντικτύπου.

[Υπογραφή]